

Michele M. Fleming
Chief Compliance Officer
mfleming@cls-bank.com

April 12, 2021

Via email

Ann E. Misback
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551
regs.comments@federalreserve.gov

Re: Notice of Proposed Rulemaking regarding Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, Request for Comments (Docket No. R-1736)

Dear Ms. Misback:

CLS Bank International ("CLS") appreciates the opportunity to comment on the *Notice of Proposed Rulemaking regarding Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers* (the "Proposed Rule"), issued by the Board of Governors of the Federal Reserve System (the "FR Board") and published in the Federal Register on Jan 12, 2021.¹

CLS was established by the private sector, in cooperation with a number of central banks, to mitigate the settlement risk (loss of principal) associated with the settlement of payments relating to foreign exchange transactions. CLS operates the world's largest multicurrency cash settlement system (the "CLS system") and provides payment-versus-payment ("PvP") settlement in 18 currencies directly to over 70 members, some of which provide access to the CLS system for over 25,000 third-party institutions.

As an Edge Act corporation established under Section 25A of the Federal Reserve Act, CLS is regulated and supervised by the FR Board and the Federal Reserve Bank of New York ("FRBNY") (collectively, the "Federal Reserve"). Additionally, the central banks whose currencies are settled in the CLS system have established the CLS Oversight Committee, organized and administered by the Federal Reserve pursuant to the *Protocol for the Cooperative Oversight Arrangement of CLS*,² as a mechanism to carry out the central banks' individual responsibilities to promote safety, efficiency, and stability in the local markets and payments systems in which CLS participates.

As a systemically important financial market infrastructure ("FMI"), CLS is subject to the CPMI-IOSCO *Principles for financial market infrastructures* (the "PFMI"), as applicable to payment systems. In addition, CLS was designated a systemically important financial market utility ("DFMU") by the Financial Stability Oversight Council in July 2012 under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Dodd-

¹ 86 Fed. Reg. 2299

² https://www.federalreserve.gov/paymentsystems/cls_protocol.htm.

Frank Act"). The FRBNY conducts day-to-day supervision of CLS, as delegated by the FR Board and CLS is subject to the risk management standards set forth in Regulation HH.

* * *

Under the scope set forth in the Proposed Rule, CLS is a "banking organization" subject to the proposed requirement to notify the FR Board of a "notification incident". As such, CLS's comments focus primarily on the details of this requirement and are directed to specific areas where CLS believes it can provide useful input.

Q1: How should the definition of "computer-security incident" be modified, if at all? For example, should it include only occurrences that result in actual harm to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits? Should it include only occurrences that constitute an actual violation of security policies, security procedures or acceptable use policies?

CLS notes the proposed definition of "computer-security incident" and welcomes the alignment with the National Institute of Standards and Technology (NIST) terms and definitions. CLS believes the definition may be too broad and it should be clarified that non-material violations of policies and procedures or policy dispensations are excluded. CLS believes the definition could be further enhanced to clarify that "near miss incidents" are not considered as in scope of "computer-security incidents" for the purposes of the Proposed Rule.

Q2: How should the definition of "notification incident" be modified, if at all? For example, instead of "computer-security incident," should the definition of "notification incident" refer to other NIST terms and definitions, or another recognized source of terms and definitions? Should the standard for materially disrupt, degrade, or impair be altered to reduce potential redundancy between the terms or to consider different types of impact on the banking organization? Should the definition not include language that is consistent with the "core business line" and "critical operation" definitions included in the resolution-planning rule? Should those elements of the definition only apply to banking organizations that have resolution planning requirements?

CLS believes that banking organizations, and in particular, FMI, have access to sufficient information to identify "core business lines" and "critical operations" in line with the proposed definition of a "notification incident". In fact, DFMUs subject to Regulation HH are already required to identify their "critical operations and services"³ related to payment, clearing and settlement.

Importantly, CLS notes that banking organizations should not be required to, under the Proposed Rule, publicly disclose which of their systems support "core business lines" and "critical operations" to avoid inadvertently inviting attacks from malicious adversaries.

In terms of the definition of a "notification incident", the Proposed Rule uses the example of a large-scale distributed denial of service attacks that disrupt customer account access for "for an extended period of time (e.g., 4 hours)". CLS requests further clarification as to whether this should be considered a set trigger which would require notification or alternatively an example of what a material outage duration could potentially look like.

³ See 12 CFR 234.3(a)(3)(iii)(A). All FMIs are expected to identify their critical operations and services in accordance with PFMI Principle 3, Key Consideration 4. See also CPMI-IOSCO, *Recovery of financial market infrastructures* (Oct. 2014) (the "CPMI-IOSCO recovery guidance") § 2.4.2 ("An FMI should identify those services it provides that are critical"); § 2.4.3 ("In general, a systemically important FMI's payment, clearing, settlement or recording functions will be regarded as critical").

Q3: How should the 36 hour timeframe for notification be modified, if at all, and why? Should it be made shorter or longer? Should it start at a different time? Should the timeframe be modified for certain types of notification incidents or banking organizations (for example, should banks with total assets of less than \$10 billion have a different timeframe)?

CLS notes the proposal that notification be required within 36 hours of a reasonable determination of an event. Given that markets settle T+1, CLS suggests that the Agencies⁴ consider a time period that is more synchronous with BAU settlement activity (i.e., 24 hours or 48 hours).

Q4. Is the proposed requirement that banking organizations and bank service providers notify the appropriate party when they “believe in good faith” that they are experiencing or have experienced a notification incident or computer-security incident, as applicable, sufficiently clear such that banking organizations and bank service providers understand when they should provide notice? How should the “believes in good faith” standard be modified, if at all? For example, should the standard be “reasonably believes” for either banking organizations or bank service providers?

Bank service providers typically require more specific contractual language in order to act upon. CLS suggests that bank service providers notify the appropriate party when they are “aware” that they are experiencing or have experienced a notification incident that impacts the services under the contract or contractual obligations.

Q5. How should notification by banking organizations under the proposed rule be provided to the agencies? Should the agencies adopt a process for joint notification to the agencies in cases where multiple affiliates of a banking organization have notification requirements to different agencies? If so, how should joint notification be done and why? Should the agencies adopt centralized points of contact to receive notifications or should notifications be provided to regional offices (such as Federal Reserve Banks) or banking organization-specific supervisory teams?

CLS requests further clarification with regards to the content of the notification the Agencies would expect to receive relating to a “notification incident”. While CLS notes that the Proposed Rule states “agencies expect only that banking organizations share general information about what is known at the time”, to provide a clear, appropriate, and realistic approach, CLS recommends that the Agencies clarify further their expectations in terms of both scope and level of detail.

CLS proposes that notifications should be provided to CLS’s Supervisors.

6. The proposed rule’s definition of “banking organizations” and “bank service providers” would include the financial market utilities (FMUs) that are chartered as a State member bank or Edge corporation, or perform services subject to regulation and examination under the BSCA. Are there unique factors that the agencies should consider in determining how notification requirements should apply to these FMUs? For designated FMUs for which the Board is the Supervisory Agency under Title VIII of the Dodd-Frank Act, would notification requirements best be conveyed through this proposed rule or through amendments to the Board’s Regulation HH?

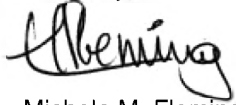
CLS proposes that the notification requirements be conveyed through this Proposed Rule as opposed to amendments to the FR Board’s Regulation HH.

* * *

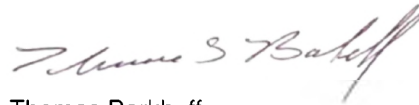
⁴ The Office of the Comptroller of the Currency (OCC), Treasury; the Board of Governors of the Federal Reserve System (FR Board); and the Federal Deposit Insurance Corporation (FDIC).

We appreciate the FR Board's consideration of the views set forth in this letter and would welcome the opportunity to discuss any of these comments in further detail, as needed.

Sincerely,



Michele M. Fleming
Chief Compliance Officer



Thomas Barkhuff
Chief Information Officer

cc: Mark Houseago, Head of Enterprise Resilience
Jason Mull, Chief Info Security Officer
Craig Rubin, Senior Legal Counsel